UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:	)	Chapter 11
FRONTIER COMMUNICATIONS CORPORATION, *et al.*,	)	Case No. 20-22476 (MG)
Reorganized Debtors.	)	(Jointly Administered)

ORDER DENYING FRONTIER'S MOTION *IN LIMINE* TO EXCLUDE CLAIMANT NOTICES AND RECORDS

Pending before the Court is Frontier's motion *in limine* ("Motion") seeking an order from this Court holding as inadmissible as hearsay the emails and related records generated by the claimants' agents alleging copyright infringement on Frontier's network. Both the RCCs and MCCs submitted responses ("RCC Response" and "MCC Response," respectively), and Frontier submitted a reply ("Reply").[1] For the following reasons, Frontier's Motion is **DENIED**.

I. BACKGROUND

According to Frontier, the RCCs and MCCs seek to use notices generated by their agents, OpSec and Maverickeye (respectively), as evidence of repeat infringement by Frontier's subscribers. (Motion at 1, 2.) These notices are automatically generated by operation of the agents' software (*id*. at 5), and feature the signatures of one of the agents' employees (*id.* at 3–4). The agents also create "evidence packages" describing their actions in generating a given notice. (*Id.* at 5.) Even though the notices were automatically generated by operation of computer software, Frontier moves to exclude them and their accompanying evidence packages on hearsay grounds. Frontier's primary argument is that the notices are fraudulent, because all of the notices

[1] The papers were submitted to the Court via email, with all parties CC'd.

purport to have been "prepared and sent by a real, live person"—the signatory of the given notice—and contain the supposed declarant's "good faith belief" that the alleged unauthorized copying of copyrighted materials "does not constitute fair use" and is not authorized by law. (*Id.* at 9.) Frontier cites to a handful of cases for the proposition that computer-generated records are hearsay when offered for their truth, and that the notices are hearsay because, despite being software outputs, they reflect "choices and inputs" made by human beings working for the agents. (*Id.* at 9–11.) Frontier also argues that the notices are not admissible under the business records exception to the rule against hearsay because the notices are prepared for use in litigation and hence are not business records. (*Id.* at 11–12.) Frontier also points to what it views as evidence of the notices' inherent unreliability: while each notice is signed, "it is totally unclear what, if anything," the signatory "or any other person had to do with these statements" in the notices, per Frontier. (*Id.* at 13.) Because there are "no indicia of trustworthiness to support the statements made in these notices," Frontier argues that *no* hearsay exception can apply.

The RCCs and MCCs disagree. The RCCs explain OpSec's process for creating notices: "(i) search BitTorrent for potentially infringing files; (ii) download a file and confirm it is infringing; (iii) collect evidence on users distributing an infringing file; and (iv) send notices to users' ISPs."[2] (RCC Reply 4.) During the process, OpSec creates a record of the work completed; this record is called an "Evidence Package." (*Id.* at 5.) Each Evidence Package contains seven files OpSec automatically generates at the time OpSec detects the infringing

[2] This process is broken down in further detail in Exhibit 1 to the RCCs' Response, an affidavit submitted by a senior OpSec employee. There is no indication in the record presently before the Court that OpSec's operations were anything but fully automated. During the pre-petition claims period (May 2, 2019 to March 10, 2020) and the administrative claims period (April 14, 2020 to April 30, 2021), OpSec sent a total of 31,724 infringement notices to Frontier on behalf of both UMG and RIAA. (Ex. 1 to RCCs' Response, ¶ 54.)

Additional details about the RCCs' agents' approach to identifying infringing content can be found in the pre-trial witness statement of Jeremy Landis, Senior Vice President at the Recording Industry Association of America (RIAA), attached as Exhibit 2 to the RCCs' Response.

activity. (*Id*.) In the fourth step, OpSec's computer system automatically generates a notice and sends it to the ISP associated with the IP address which OpSec has automatically tied to potential infringement. (*Id.* at 6.) OpSec's software draws the information for the notice directly from the Evidence Package. (*Id.*) Each Notice contains the information required by the DMCA, and so includes the signature of an OpSec employee in a managerial role; these signatures are automatically generated without human intervention on a per-notice basis, and the signatory attested to each Notice based on their understanding and oversight of OpSec's infringement detection and notice submission process. (*Id.*) The RCCs argue that, given the above, the data generated by a computer—the notices and Evidence Packages—are *not* hearsay, pursuant to multiple court decisions on similar facts, since they are machine-generated and hence not "statements"; the RCCs encourage the Court to follow the Fourth Circuit's decision in *BMG v. Cox*, 881 F.3d 293 (4th Cir. 2018), and hold that notices are computer-generated and not "statements" subject to the rule against hearsay, despite the fact that the notices bear signatures. (*Id.* at 10.) All the Federal Rules of Evidence require for admission is a sufficient foundation to show that the agents' systems reliably generate notices. (*Id.* at 9–10.) As for Frontier's contention that the signatures somehow make the notices fraudulent, according to the RCCs, that is not right: a "senior OpSec employee authorizes the OpSec system to affix their signature to each Notice based on their understanding and oversight of the operation of OpSec's system." (*Id.* at 10.) That employee's attestation under penalty of perjury in each notice is limited to the statement that the agent "is authorized to act on behalf of" the rightsholder "in matters involving the infringement of their sound recordings, including enforcing their copyrights and common law rights on the Internet," which is all the DMCA requires. (*Id.*) As for the Evidence Packages, they are also computer-generated and hence not hearsay. (*Id.* at 11.)

Even if the notices and Evidence Packages are hearsay, the RCCs argue that they should enter the record under the business records exception, as business records of the agents. Frontier's argument that the documents were created for the purpose of litigation and therefore are outside the scope of this exception falls flat because the "RCCs sent Frontier Notices to try to get Frontier to do something about the rampant copyright infringement on Frontier's network, not for litigation purposes," and litigation "entered the picture only after analysis of the Notices and other evidence revealed that Frontier had not taken necessary action against known repeat infringers." (*Id.* at 14.) Finally, the RCCs argue that the notices are admissible for the non-hearsay purpose of showing that Frontier "knew about the infringement on its network that the Notices detail." (*Id.* at 17.)

The MCCs filed a joinder in which they second all of the RCCs' legal arguments. (MCC Response at 6.) They also explain the operation of their agent's, Maverickeye's, software, which seems to be substantially similar to how the RCCs' agent works: the agent searches "for torrents . . . pirating" a particular copyright-protected work; two employees of the agent independently verify the system's identification of a copyrighted work; and upon verification, the system automatically generates a notice to be sent to the ISP associated with the IP address at which the apparent copyright infringement occurred. (*Id.* at 2–3.) The key difference is the second step, when two employees independently verify the system every time it identifies a copyrighted work; from the record presently before the Court, it does not seem that OpSec's process features this degree of human involvement. The MCCs also argue that Frontier is judicially estopped from arguing that the notices cannot be admitted under the business records exemption because they were prepared for use in litigation, because Frontier previously argued (in briefing concerning the MCCs' spoliation motion) that the notices did *not* suffice to put Frontier on

notice of potential litigation. (*Id.* at 5–6, *see also id.* at 7–8 ("Frontier's argument that the DMCA Notices at issue are not admissible because they were supposedly prepared in anticipation of litigation is inherently inconsistent with its prior position that these same Notices did not provide it with notice that it should preserve its records.")

In its Reply, Frontier doubles down on its argument that the notices *are* human-created statements, relying on the signatures of the agents' employees. Because the notices "purport to be statements signed by individuals making certain representations about the underlying data," they are not the "raw data printouts" or the like which have previously been recognized to be computer-generated documents and hence not hearsay (because not a "statement"). (Reply at 2–3.) In Frontier's view, any "human involvement, oversight, and authorization" renders the notices "textbook hearsay." (*Id.* at 3–4.) Frontier also repeats its argument that the notices were "created with litigation in mind" and therefore cannot be trusted because they were not generated in the ordinary course of business. (*Id.* at 4–5.) Frontier claims that "the RCCs undisputedly launched a campaign *at Frontier* with the express and intended purpose of forcing Frontier to take certain actions; the notices were thus not generated in the ordinary course of the RCCs' businesses or OpSec's, *but with the aim of building a self-serving record*." (*Id.* at 5.) (Frontier applies the same argument to the MCCs, *id.* at 6.)

Frontier then adds an argument: it claims that the notices and Evidence Packages "talk past each other," because "the notices make sweepingly broad conclusions—that a Frontier subscriber engaged in copyright infringement—when the evidence packages show no such thing," but just show "that the Claimants' agents downloaded pieces of files they were authorized to download." (*Id.* at 7.) As for the RCCs' argument that the notices can be submitted for a non-hearsay purpose, Frontier agrees, but it insists that the non-hearsay purpose

cannot be that Frontier knew of infringing activity, as that would presume the truth of the notices. (*Id.* at 8.) Finally, Frontier denies that it took contradictory stances in this litigation: "There is no inconsistency between Frontier's current position that the *MCCs* had a litigation purpose in generating their notices . . . and its prior argument that receipt of the notices did not cause *Frontier* to anticipate litigation, giving rise to a duty by Frontier to preserve documents." (*Id.* at 9.)

The language of the notices provided by Frontier and the plaintiffs as attachments to their briefing is instructive. One form email, from Debra Giddings of OpSec on behalf of the RCCs, states that, "[u]nder penalty of perjury, we submit that the RIAA is authorized to act on behalf of its member companies in matters involving the infringement of their sound recordings, including enforcing their copyrights and common law rights on the Internet." (Motion Ex. 1.) Another email sent by an agent of the MCCs, signed by Anna Reiter from Copyright Management Services, states, "[u]nder penalty of perjury, I assert that Copyright Management Services, Ltd. (CMS) is authorized to act on behalf of the owner of the exclusive copyrights that are alleged to be infringed herein . . . . We have a good faith belief that use of the copyrighted material detailed above is not authorized by the copyright owner, its agent, or the law. In addition we have a good faith subjective belief that the use does not constitute fair use. The information in this notice is accurate and we state, under penalty of perjury, that we are authorized to act on behalf of the owner of the copyright that is allegedly infringed." (Motion Ex. 2; *see also id.* Ex. 4 (identical language in a form email signed by Catherine Hyde from PML Process Management); Ex. 6 (email on behalf of one of the MCCs, signed by Carl Crowell of Crowell Law, which states, "Under penalty of perjury I verify: The below information accurately identifies the observed time of infringing activity, IP address used, port used, and the specific

content including Rights Holder (owner), title, file name and file has; I am fully authorized to act on behalf of the owner of an exclusive right that is allegedly infringed; I have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.")).

II. LEGAL STANDARD

A "statement" is defined by Federal Rule of Evidence[3] ("FRE") 801(a) as an "(1) oral or written assertion or (2) nonverbal conduct of a *person,* if it is intended by the person as an assertion." Hearsay is defined as "a *statement,* other than one made by the *declarant* while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FRE 801(c) (emphases added). "A declarant is a *person* who makes a statement." FRE 801(b) (emphasis added). Only a *person* may be a declarant and make a statement. Accordingly, "nothing 'said' by a machine . . . is hearsay." 4 Mueller & Kirkpatrick, *Federal Evidence,* § 380, at 65 (2d ed. 1994). *See United States v. Hamilton,* 413 F.3d 1138, 1142–43 (10th Cir. 2005) (concluding that the computer-generated header information accompanying pornographic images retrieved from the Internet was not a hearsay statement because there was no "person" acting as a declarant); *United States v. Khorozian,* 333 F.3d 498, 506 (3d Cir. 2003) (concluding that an automatically-generated time stamp on a fax was not a hearsay statement because it was not uttered by a person); *United States v. Hall*, 497 F. App'x 299, 300 (4th Cir. 2012) (results of intoximeter exam are not hearsay because machine-generated); *United States v. Washington,* 498 F.3d 225, 231 (4th Cir.2007) ("[R]aw data generated by [ ] machines do not constitute 'statements,' and the machines are not 'declarants' . . . . Accordingly, nothing said by a machine is hearsay."); *United States v. Waguespack*, 935 F.3d 322, 333–34 (5th Cir. 2019) (holding that

[3] Made applicable to bankruptcy proceedings by Federal Rule of Bankruptcy Procedure 9017.

results of investigation into child pornography distribution over the Internet, which was conducted via BitTorrent program which tracks IP addresses which recently shared child pornography and creates activity logs, was not hearsay because the results were machine-generated materials and not the statements of a witness); *United States v. Ballesteros*, 751 F. App'x 579, 579–80 (5th Cir. 2019) (determining that the output of a computer program which tracked defendant's location via GPS tracking of his cellphone was not a "statement" made by a "person" and hence not hearsay); *United States v. Lamons*, 532 F.3d 1251, 1263–64 (11th Cir. 2008) (concluding that a computer-generated spreadsheet of telephone billing data was not hearsay); *Patterson v. City of Akron*, 619 F. App'x 462, 479–80 (6th Cir. 2015) (holding that a Taser report was "merely a report of raw data produced by a machine" and thus did not constitute hearsay).

"Any concerns about the reliability of such machine-generated information is addressed through the process of authentication[,] not by hearsay or Confrontation Clause analysis. When information provided by machines is mainly a product of 'mechanical measurement or manipulation of data by well-accepted scientific or mathematical techniques,' . . . reliability concerns are addressed by requiring the proponent to show that the machine and its functions are reliable, that it was correctly adjusted or calibrated, and that the data . . . put into the machine was accurate . . . . In other words, a foundation must be established for the information through authentication, which Federal Rule of Evidence 901(b)(9) allows such proof to be authenticated by evidence 'describing [the] process or system used to produce [the] result' and showing it 'produces an accurate result.'" *United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (internal citations omitted).

FRE 802 states that hearsay is not admissible unless a federal statute, the FRE, or other rules prescribed by the Supreme Court provides otherwise. FRE 803(6) sets out the "business records" exception to the rule against hearsay, and provides that "the following are not excluded by the rule against hearsay, regardless of whether the declarant is available as a witness":

> (A) the record was made at or near the time by — or from information transmitted by — someone with knowledge;
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
> (C) making the record was a regular practice of that activity;
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and
> (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.

Rule 803(6) allows business records to be admitted "if witnesses testify that the records are integrated into a company's records and relied upon in its day to day operations." *Matter of Ollag Constr. Equip. Corp.*, 665 F.2d 43, 46 (2d Cir. 1981). "This Circuit has recognized that a custodian who testifies as to the authenticity of a record need not have firsthand knowledge of the creation of the record." *United States v. Reyes*, 157 F.3d 949, 952 (2d Cir. 1998).

"Rule 803(6) 'favor(s) the admission of evidence rather than its exclusion if it has any probative value at all.'" *Matter of Ollag Const. Equip. Corp.*, 665 F.2d at 46 (internal citation omitted).

III. DISCUSSION

First, it is not immediately clear whether the plaintiffs wish to use the notices as evidence of actual, proven infringement, or if they wish to use the notices as evidence of credible allegations of infringement which Frontier may have been obligated to act upon under the DMCA. The language of the notices suggests that the latter is more likely to be the case, as the form language in each notice provided to the Court for review with these papers states clearly

that the sender only has a "good faith belief" that there was infringement, or emphasizes that the infringement was "alleged[]." (*See supra* for excerpts of notices.)

Second, the notices are obviously computer-generated, given the unchallenged testimony provided by the RCCs,[4] the sheer volume of notices, and their distinctly repetitive and vague language. The signatories did not draft each and every notice. Moreover, the signatories of the notices provided thus far to the Court only made specific statements under penalty of perjury, to the effect that the agent was authorized to act on behalf of the copyright-holder, that the notice accurately identifies certain information gathered by the agent, and that the agent has a "good faith *belief*" that infringement occurred. (*See supra*.) Nowhere do the signatories testify on penalty of perjury that *infringement actually occurred*. It is entirely possible for one employee of one of the agents to have sufficient knowledge of the agent's relationship with the copyright-holder and the operations of the agent's software such that they can testify on penalty of perjury that the agent is authorized to work on behalf of the rightsholder, that the notice accurately captured what the agent's software identified on the Internet, and that such information captured by the agent's computer would give rise to a good faith belief that infringement occurred as flagged by the software. Frontier's argument that the notices are somehow inherently false therefore fails, as it rests on a poor reading of the language of the notices. (Relatedly, Frontier's argument that the Evidence Packages somehow contradict the notices also fails, for the same reason: despite Frontier's claim that the notices "make sweepingly broad conclusions—that a Frontier subscriber *engaged in* copyright infringement," they do not do so. They only state that there is reason to have a good faith *belief* that such infringement occurred, and such a belief seems adequately supported by the content of the Evidence Packages and the signatories'

[4] *See* Exhibits 1, 2 to the RCCs' Response.

understanding of how the agents' infringement-identifying processes work. (Reply at 7; *see also* RCC Response at 5–6 (describing contents of an Evidence Package).))

The key question here is whether the notices provided by the plaintiffs' agents are the kinds of computer-generated documents that are not "statements" so cannot be hearsay. *BMG*, 881 F.3d at 313. The Court concludes that those created by OpSec are *not* hearsay, but those created by Maverickeye *may be* hearsay. However, even if they are hearsay, the notices created by Maverickeye can enter the record pursuant to the business records exception to the rule against hearsay.

A. OpSec

OpSec's infringement-identifying process features very little, if any, human involvement. (*See* RCC Response, Ex. 1, ¶¶ 28–51 (trial witness statement of Jason Allen, Senior Manager at OpSec, describing process).) The notices were automatically generated by OpSec's computer systems and include information gathered by OpSec's computers, as well as information required under the DMCA, including a signature. (*Id.* ¶ 49.) As the RCCs explain, "[t]hese signatures were generated on an automated basis without human intervention on a Notice-by-Notice basis." (RCC Response at 6.) Frontier does not challenge this statement.

Frontier's argument that there can be no such thing as an entirely computer-generated document which also contains the signature of a human without that document somehow being fraudulent fails. The notices, including the signatures, were automatically generated. This does not mean that the signatories *cannot* swear to the *specific claims* they made under penalty of perjury in each notice, despite having not personally reviewed every notice. The above excerpts make clear that those claims were universally applicable across notices, regardless of their exact content. The signatories swore that the agent was authorized by their client to act on the client's

behalf, which is a fact unrelated to the content of any particular notice; and that, in essence, they knew how their computers operate and trusted them to accurately capture certain information from the Internet, and because of their knowledge of the computers' operations, had a good-faith belief that such information gives rise to an inference of copyright infringement. Such statements are not so particularized that the signatory would need to know the exact contents of each of the form notices to swear to such statements. The signatories were functionally swearing to the *reliability* of the machine-generated information and the limited inferences to which such information gives rise, given how the machines are programmed. There is no indication that the signatories independently verified the exact content of every single notice—the opposite seems to have been the case. This is therefore a far cry from the degree of human involvement which compelled the Eighth Circuit in *United States v. Juhic* to determine that a computer-generated spreadsheet tracking files a particular testifying officer believed to be child pornography contained hearsay: "While the reports may have been computer-generated, human statements and determinations were used to classify the files as child pornography. It was only after a human determined that a file contained child pornography that the [relevant information] was inserted into the computer program . . . . The human involvement in this otherwise automated process makes the notations hearsay." 954 F.3d 1084, 1086–88 (8th Cir. 2020). Unlike in *Juhic*, here, no individual determined that each notice and accompanying evidence package reflected an instance of copyright infringement.

Everything presently before the Court indicates that OpSec's notices and accompanying evidence packages are solely machine-generated results which do not include or reflect statements of human beings. These results of a fully-automated Internet-scraping process are

closest to the "raw data" outputs which courts have repeatedly held are *not* statements and therefore do not qualify as hearsay. *See supra*.

The Fifth Circuit in *Waguespack* assessed a remarkably similar Internet-scraping process and determined that the resulting report was machine-generated and therefore not hearsay. That case, which concerned a criminal defendant's Confrontation Clause challenge to the admission of the report, concerned a child pornography investigation. The investigator used "Torrential Downpour," described as "a BitTorrent program used by law enforcement to investigate peer-to-peer networks" which "targets IP addresses that have recently shared child pornography and creates an activity log of the files involved," to track down the downloads of certain images to particular IP addresses. 935 F.3d at 327. This technology sounds nearly identical to the infringement-identifying process used by OpSec and Maverickeye, which also use BitTorrent to identify certain Internet users who seem to be sharing files identical to those which the agents have confirmed are copyright-protected. (*See* RCC Reply at 4–5.) The investigator in *Waguespack* traced an IP address to a particular residence, at which point officers executed a search warrant there, seized a computer in the defendant's room, and found on it "software actively searching for and downloading files with file names indicative of child pornography." *Waguespack*, 935 F.3d at 327. The defendant raised a Confrontation Clause objection to the admission of child pornography images downloaded by the investigator and the investigator's accompanying Torrential Downpour logs, because the prosecution's failure to call the investigator in its chase-in-chief violated the defendant's right to confront the witness. *Id.* at 332. The Fifth Circuit ruled against the defendant, holding that the forensic report was "machine-generated" and hence not a statement of a witness and did not trigger the Confrontation Clause. *Id.* at 334. The analysis would be identical under a hearsay objection. *Id.*

(citing to a case concerning a hearsay objection to a machine-generated report). The Fifth Circuit's well-reasoned decision in *Waguespack* is persuasive in this context, which involves a very similar and entirely automated investigation process, at least as applied to OpSec. And of course, the Fourth Circuit's decision in *BMG v. Cox*, which dealt with virtually identical facts, is also highly persuasive: there, the Fourth Circuit held there that notices sent on behalf of copyright owners to an ISP were "not hearsay because [they] were generated by a computer and thus" were not "statements," and contrary to the ISP's argument (identical to that of Frontier here), "the fact that the machine-generated notices also contained the signature of Rightscorp's CEO and an oath under penalty of perjury does not transform them into statements, since the information itself was not prepared or created by a human." 881 F.3d at 313.

The cases Frontier cites to the contrary are inapposite. In *United States v. Bonomolo*, 566 F. App'x 71 (2d Cir. 2014), computer-generated spreadsheets detailing grants given to various schools and students were allowed into evidence pursuant to the business records exception to the hearsay rule, but it is not clear from the opinion whether the argument that computer-generated records are *not* statements was even considered, nor is it clear how the spreadsheets were created (e.g., whether the underlying documents—statements concerning grant amounts—were created by people and the spreadsheets were mere compilations of human-made statements). *United States v. Hayes*, a non-binding Tenth Circuit case from 1998, concerned IRS computer records which appear from the opinion to be compilations of individuals' tax filings. 861 F.2d 1225, 1228 (10th Cir. 1998). These, too, were admitted under the business records exception, but there was no in-depth discussion of how the computer records were created (nor if they were, like the spreadsheets, mere compilations of man-made documents), and nothing in the opinion suggests that the argument this Court is presented with (whether computer-generated

documents are statements) was considered.[5] The same goes for *UMG Recordings, Inc. v. Grande Commc'ns Networks*, No. 1:17-cv-00365, 2023 WL 11938218, at *14 (W.D. Tex. May 11, 2023), *aff'd in part and vacated in part*, 118 F.4th 697 (5th Cir. 2024) (overruling an objection to Rightscorp's[6] copyright infringement notices on hearsay grounds, noting that the notices were admitted "after a proper foundation was laid to qualify the notices as business records," but not considering other arguments); *UMG Recordings, Inc. v. Grande Commc'ns Networks, LLC*, 384 F. Supp. 3d 743, 762 (W.D. Tex. 2019) (similar); and *Dish Network L.L.C. v. Fraifer*, No. 8:16-CV-2549-TPB-CPT, 2023 WL 8622142, at *6 (M.D. Fla. Aug. 31, 2023), *report and recommendation adopted*, No. 8:16-CV-2549-TPB-CPT, 2024 WL 51035 (M.D. Fla. Jan. 4, 2024) (similar). The portion of the Second Circuit's decision in *Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.*, 38 F.3d 627, 632 (2d Cir. 1994), which Frontier cites (Motion at 9), discussed instances where data stored electronically *could be* business records—i.e., fleshed out one type of business record—but did *not* opine more broadly on all the various rationales on which computer records could be admitted into evidence. The same goes for the cited excerpt of *Cap. Marine Supply v. M/V Rolland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983) (focusing on "[c]omputer *business records*," not computer-generated documents writ large).

In short, OpSec's notices and accompanying Evidence Packages are machine outputs and are *not* statements, so are not hearsay.

---

[5] By contrast, we know that OpSec's records are entirely computer-generated. *See supra*; *see also* Exhibit 1 to the RCCs' Response.

[6] From descriptions in other opinions, Rightscorp seems to be a similar infringement-tracking agent as the ones discussed by the parties in this case. *See, e.g.*, *UMG Recordings, Inc. v. Grande Commc'ns Networks, LLC*, 384 F. Supp. 3d 743, 762 (W.D. Tex. 2019) (discussing operations of Rightscorp).

B. Maverickeye

There is one crucial difference between OpSec's approach and Maverickeye's, which is that, per the MCCs' brief, Maverickeye's investigative process *does* involve human input: to confirm that the file identified by Maverickeye is in fact a work in which one of Maverickeye's clients has a copyright, "[t]wo people at [Maverickeye] independently verify" that the identified work "is a copy of the copyright protected Work." (MCC Response at 2; *see also* Exhibit A to MCC Response (Declaration of Thomas Nowak, CEO of Maverickeye) ¶ 35.) Under the logic of *Juhic*, this could very well render the notices generated by Maverickeye statements made by real people. *See Juhic*, 954 F.3d at 1086 (classifying computer-generated reports of child pornography downloads as hearsay because "[i]t was only after a human determined that a file contained child pornography that the [relevant information] was inserted into the computer program," so "human statements and determinations were used to classify the files as child pornography").

The Court need not decide this issue, because even if Maverickeye's notices *are* hearsay, they are admissible under the business records exception, FRE 803(6). A proper foundation for admission of the Maverickeye notices and evidence packages has been laid in the Maverickeye's CEO's declaration, attached as Exhibit A to the MCCs' Response, which qualifies as custodial testimony under FRE 803(6)(d). There, the CEO explains that Maverickeye's business is to provide forensic investigation services (*id.* ¶ 7–8, 19–22), so the production of notices and evidence packages is clearly part of Maverickeye's "regularly conducted business activity" and they were not created "in response to unusual or 'isolated' events." *Phoenix Assocs. III v. Stone*, 60 F.3d 95, 101 (2d Cir. 1995). Frontier's argument that none of the notices count as business records because they were all made in preparation for litigation borders on specious: the very

cases Frontier cites admit notices in copyright infringement litigation against ISPs into evidence under the business records exception (*see supra*; *see also* RCC Response at 13 (collecting cases)), despite the fact that the noticing agents and plaintiffs in those cases would presumably be in the exact same situation as the RCCs, MCCs, and their agents are in here. Just because Maverickeye's business is to prepare documents which *may* be used in future litigation against a *then-unknown* defendant, on *then-unknown claims*, does not mean that *all* of Maverickeye's records are inherently unreliable.

For the foregoing reasons, the MCCs' agents' notices and Evidence Packages are admissible into evidence under the business records exception to the rule against hearsay.

The Court need not address the other arguments made by the parties in this round of briefing.

IV. CONCLUSION

For the foregoing reasons, Frontier's Motion is **DENIED**.

IT IS SO ORDERED.

Dated: April 3, 2025
New York, New York

/s/ Martin Glenn
MARTIN GLENN
Chief United States Bankruptcy Judge